A WW2 device for breaking the M-209 encryption machine

Magnus Ekhall
Independent Scholar
magnus.ekhall@gmail.com

Klaus Schmeh
Independent Scholar
klaus@schmeh.org

Abstract

According to an eyewitness report by German engineer Reinold Weber published in 2004, a German cryptanalysis unit broke the U.S. cipher machine M-209 in the Second World War. For this purpose, the specialists involved built an electromechanical machine ("Weber machine"), which included binary logic and bore some resemblance with the Turing Bombe. In previously unpublished documents contained in the TICOM reports, information can be found about a cryptanalysis device that is probably identical with the Weber machine. Based on the said sources, this paper describes what is known about this deciphering technology.

1 Introduction

Contrary to the Americans and the British, who concentrated their crypto activities in Arlington Hall and Bletchley Park respectively, the Germans didn't have a centralized cipher authority in the Second World War. Instead, there were about a dozen crypto units in Nazi Germany, operated by different military and civilian authorities without much interchange (Schmeh 2022). This failure in bundling cryptologic forces is today considered a major failure, which contributed to the German World War II cryptology not being as successful as its Allied counterparts.

From a historian's point of view, the fragmentation of the German WW2 crypto efforts makes this topic difficult to research, as the sources are spread to many different locations. The most important source on this topic so far is the information gathered by the TICOM (Target Intelligence Committee), an Allied project aiming to find and seize German intelligence assets, particularly in the field of cryptology and signals intelligence, starting in 1944 (Rezabek 2017). Parts of this material were declassified starting in 2010.

Even before the TICOM files became available to historians, it had been known that German cryptanalysts in World War II had achieved a number of notable successes. Among other things, they broke the U.S. tactical encryption machine M-209, which was designed by the well-known Swedish crypto entrepreneur Boris Hagelin (Leiberich, 1996).

Figure 1. The M-209 was used by the U.S. military for encrypting tactical communication during the Second World War. Source: Cryptomuseum

The M-209 can be regarded as a device that produces a key-dependent pseudo-random sequence (Reuvers 2022b). For encryption, the plaintext is added to this sequence; for decryption, the sequence is subtracted from the ciphertext. The M-209 is a variant of Hagelin's C-38 cipher machine, and it works similarly as the other Hagelin C machines, such as the C-36 and the C-52 (Reuvers 2022a). It uses a key consisting of three parts:

- *Cipher wheel settings*: The M-209 includes six letter wheels that can be set like a combination lock. The setting of these wheels was used as a short-time key, which was changed frequently.
- *Pin settings*: Each cipher wheel comprises a pin for each letter. Each of these pins can be activated or deactivated. Changing this part of the key is more laborious than setting the cipher wheels.
- *Lug positions*: An M-209 includes a drum, on which lugs can be positioned. This part of the key was typically used as a long-term key.

For the cipher wheel settings to be changed, the case of an M-209 device needs to be open, while the machine as such can be closed (War Department 1944). The pin settings and the lug positions, on the other hand, require the machine itself to be opened, too. For this reason, the cipher wheel settings can be regarded as an "external setting", while the pin settings and the lug positions represent the "internal settings".

2 The keying procedure

The M-209 was employed with a keying protocol that ensured that an enemy cryptanalyst had only access to a small amount of ciphertext encrypted with the same key. (War Department 1944) and (Barret 1943) provide information about this procedure.

Another description was created by German cryptologist Alfred Pokorn from OKH/Chi (TICOM 1945b). OKH stands for "Oberkommando des Heeres" ("Army High Command"), while "Chi" is an abbreviation of "Chiffrierabteilung" ("Cipher Department"). Alfred Pokorn might be identical with the author of the books "Pfadfinder-Handbuch" (Pokorn 1950) and "Apatschen-Indianer" (Pokorn 1960). His description is presented in the following:

"When ciphering, the pins and lugs had to be set according to key list and date – 'internal setting', the wheels were turned to any chance position – 'external setting' – and the letters then showing on the wheels were used for the 3rd to 8th letter of the external indicator of the message to be sent. Then any letter of the alphabet was printed several times, this clear letter being used as the first 2 letters of the external indicator. The first letters of the cipher text produced by this printing, were then [set] on the wheels. As only one of the wheels bears all the letters of the alphabet, usually more than 6 letters had to be printed to provide letters suitable for all the wheels. After that, the ciphering could begin."

This means that enciphering a message started with configuring the M-209 according to the daily key by setting the pins on the wheels and the lugs on the drum ("internal setting"), as indicated on some list. Then the sender randomly selected a starting position for the six wheels, say ABCDEF. He then repeatedly enciphered a random letter, say X, and received an output, say GHIJKL ("external setting"). The operator then set the wheels of the M-209 to GHIJKL and started to encipher the actual message. The message indicator in this example would be: XXABC DEFYZ, where YZ designates the cipher key list used.

As Pokorn mentions, the internal setting was changed according to a key list and the date. Most likely the internal setting was changed daily and constitutes a common "daily key" which is shared between all M-209 operators on a given network and period of time. The purpose of the keying procedure is to allow different external settings to be used for each message that is sent. The message indicator, which is transmitted in the clear, can easily be used by the receiving cipher clerk to get the correct external setting for the message in question thus allowing for deciphering of the message. But if you do not know the internal setting, the message indicator is useless.

It is possible for a cryptanalyst to manage to find an internal setting and external setting that correctly deciphers an M-209 message but at the same time not knowing the corresponding letters of the cipher wheels. In this case only this particular message can be deciphered since the absence of the true external setting prevents using the message indicator of other messages. When this situation occurs, it is said that the cryptanalyst has produced a "relative key or setting". If however the true external setting has been found, thus allowing the deciphering of all messages from that network and date, it is referred to as the "absolute key or setting".

3 Reinold Weber's report

In September 2004, the German online magazine Telepolis published an article telling the story of Reinold Weber (1920-2021), who worked as a codebreaker in the Second World War (Schmeh, 2004). In the following, the main facts from this publication are provided. As a caveat, it must be taken into account that Weber's report, which was recorded six decades after the events described, might contain errors. One of the reviewers of this paper has made the authors aware of additional sources that can be used to verify Weber's account. While this task is not within the scope of this work, it is well possible that Weber exaggerates his role in the codebreaking work he was involved in.

According to his report, Weber started his service in Louveciennes near Paris, France, working for a codebreaking unit he remembers as being named FNASt 5. A reviewer told us that Weber probably remembered wrong, and that he instead meant NAASt 5.

According to Weber, his first cryptanalytic success was the breaking of a U.S. code referred to as "TELWA code" by the Germans. This system was later identified as the War Department Telegraph Code, also known as SIGARM (Schmeh 2015). Weber's success (which was rated as exaggerated by a reviewer) earned him recognition among his codebreaking colleagues and led to his promotion to a subunit that took care of more advanced enemy ciphers. When Weber joined this group, his comrades were already able to decipher messages encrypted with the M-209 cipher machine in some cases. The breaking was a laborious and time-consuming process based on manual work only.

4 M-209 cryptanalysis

We don't know how Weber and his co-workers broke M-209 messages. However, one of the authors of this work discovered several descriptions of M-209 cryptanalysis methods in the TICOM files (TICOM undated, TICOM 1948/2), one of which is the aforementioned report by Alfred Pokorn (TICOM 1945b).

As Pokorn writes, it was necessary to first find out how the pins on the wheels and the lugs were arranged on that particular day, i.e. the internal setting had to be determined. For this purpose, one first needed to attack messages in depth, which depended on operator errors. The messages in depth could be broken linguistically, and with the clear-text available one could figure out the pin and lug settings.

At this point one knew exactly, for this particular message, what sequence of active pins had been used by the six wheels of the M-209 for every pair of ciphertext and clear-text letters. However, one did not know where in this pin sequence the letters printed on the M-209 wheels were: where in the sequence is position A, B and so on? In other words, the external setting was still unknown.

To find the external setting, a number of candidate settings were tried, working with the various pin sequences and the indicators of the messages involved and trying to get a consistent situation where the use of the message indicators sets the M-209 wheels in the right place.

For more information about the breaking of the M-209, check (Miller 1950) and (Barret 1943).

5 The Weber machine

In April 1944, Weber had, according to his report, the idea of constructing a machine that would facilitate the M-209 deciphering. This device was to consist, on the one hand, of four Bakelite rollers with slots into which punched sheet metal templates could be inserted to reproduce the relative setting. On the other hand, a relay circuit was planned with a plate above it on which flashlight bulbs marked with letters could be plugged in. The multiple switchable relays were to be soldered to each other and to the electric bulbs inside a box.

As Weber reports, he received permission to build such a machine and traveled to Berlin to ask the company Hollerith, which was later to become a part of IBM, for support. However, his inquiry was rejected, partially because Weber was not allowed to talk about the real purpose of this device.

After the U.S. Army had entered France on D-Day in June 1944, the NAASt 5 was relocated to Germany. It took its home in a former cigar factory in Krofdorf am Gleiberg north of Frankfurt. In Krofdorf there was a precision

engineering company called Dönges (today a part of Schunk Phono Systems), which had stocks of silver steel and brass as well as various machining equipment. Weber saw an opportunity to use them to now realize his machine. His supervisor agreed and allowed him to work with a colleague three days a week to build his deciphering device. Although neither of them had any experience with processing metal, the two succeeded in producing the four rollers, each with 26 slots, as well as punched sheet metal plates. In addition, a considerable number of cable connections had to be soldered.

The two decipherers were able to procure the necessary relays, each of which had to be able to establish from one to 256 connections. So, they finally created a machine consisting of two boxes: one the size of a desk, which contained the relays and the four rotating rollers, and another box with edges 80, 80 and 40 centimeters long. The latter box contained 26 by 16 bulb sockets that could be used to replicate the letters of the relative setting. By the end of August 1944, the Weber machine was operable.

According to Weber, his machine needed about seven hours to determine an absolute setting. Without machine aid, this task had lasted about a week when three people worked on it.

At the beginning of 1945, when the U.S. Army approached German territory, the NAASt 5 was relocated again, this time to Salzburg, Austria. To Weber's great surprise, his deciphering machine had also found its way there. However, the unit lacked the radio technology to intercept Allied radio messages, and so the device now proved useless. His superior therefore ordered the machine to be destroyed. With pickaxe, hatchet, hammer and steel saw, Weber then scrapped the device, the construction of which had occupied him for several months.

Until recently, the information provided in Weber's report was everything that was known about the Weber machine. No second source existed. There was no drawing or photograph of the machine.

6 The DF 114 device

In 2022, one of the authors of this paper discovered a document titled "German Cryptanalytic Device for Solution of M-209 Traffic" in the TICOM file (TICOM 1948a). This document, which we will refer to as DF 114, had been declassified in October 2010, six years after the publication of the Weber report. It describes a device used for "machine treatment of AM-1 compromised texts in depth of 5". AM-1 was the name of the M-209 used by the Germans. We'll refer to this machine as DF 114 device.

It is important to note that the TICOM reports, just like the Weber report, need to be approached with care and suspicion. Much of the information provided depends on interrogations conducted months or years after the events occurred and certainly contain errors and inaccuracies. Also, TICOM reports written by the British and US TICOM members have been found to contain factual errors, most likely due to a lack of a complete understanding of the situation when the reports were written. The reports were often based on prisoner-of-war interrogation reports, which often contained errors and incomplete information.

The DF 114 document mentions that it is a translation of a German document catalogued as TICOM 2785 item 19. To our regret, we don't have access to this source.

According to DF 114 the device consisted of three major parts: A "skip box", a distributor and a switching device. Apart from that, there were several auxiliary parts such as a lamp panel, plug-board and various power related electrical components.

The "skip" (German "Sprung") referred to in the skip box refers to how the M-209 enciphers and deciphers a letter: the clear text letter is advanced a number of steps, or skips, in a reversed alphabet in order to produce the resulting letter. This wording is also used for example in (TICOM 1948b).

The skip box contains 120 electrical switches which are spring loaded. Five cylinders are mounted above the array of switches. The cylinders can be fitted with sheet metal lugs and it is these lugs that eventually press the electrical switches when the cylinders are rotated. Each lug has six tabs that can be present or cut away. This represents the state of the six cipher wheels of the M-209 at a given position and can be directly associated with a fixed number of "skips".

The distributor is an electro-mechanical device which steps through the different combinations produced by the skip box and distributes each combination, in turn, to the switching device.

The switching device contains six test circuits, one for each wheel of the M-209. This is a circuit implemented with relays, connected as a binary tree, and lamp panels with flashlight bulbs. The purpose of the switching device is to indicate if all six test circuits conduct: a possible solution has then been found.

DF 114 has rather precise figures related to the electrical characteristics of the device. Voltages and currents are listed with up to two decimal points. Maximum current is described to be 14.31 Ampere and the maximum power consumption 448 Watt.

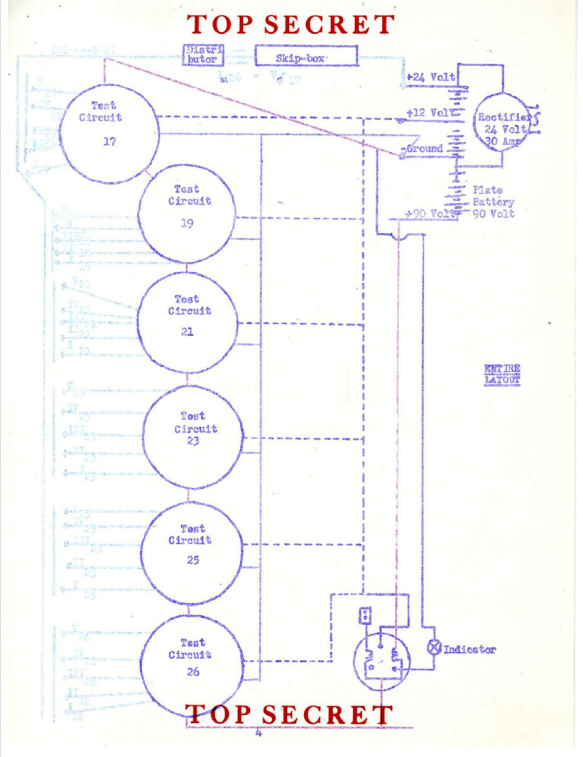

Figure 2. The document DF 114 describes an M-209 breaking machine that is probably identical with the Weber machine.

7 Are the machines identical?

Neither the Weber report nor DF 114 provide an exact description of the devices they cover. Nevertheless, it is clear that both devices served the same purpose and worked in a similar way. In addition, Weber's unit ended up in the Salzburg area, while the first page of DF 114 mentions that the document in question was found buried not far from Salzburg. This suggests that the two machines are identical.

In his report, Weber explains that his machine was used to speed up the process of finding the absolute key given a few relative keys from the same day. This might be related to what is mentioned in (TICOM undated). In other words, the problem to be solved seems to be to find the daily key given a number of message keys. In the following, we assume that the two devices are identical or at least different implementations of the same concept. According to Weber's report, his machine was destroyed by himself in early 1945, before the enemy reached the Salzburg area. This explains why the TICOM commission apparently only found a description of the Weber machine, but not a specimen of the device itself. Of course, it is also possible that several specimens of this machine existed. Perhaps, the design was copied inside the NAASt 5, even without Weber's knowledge.

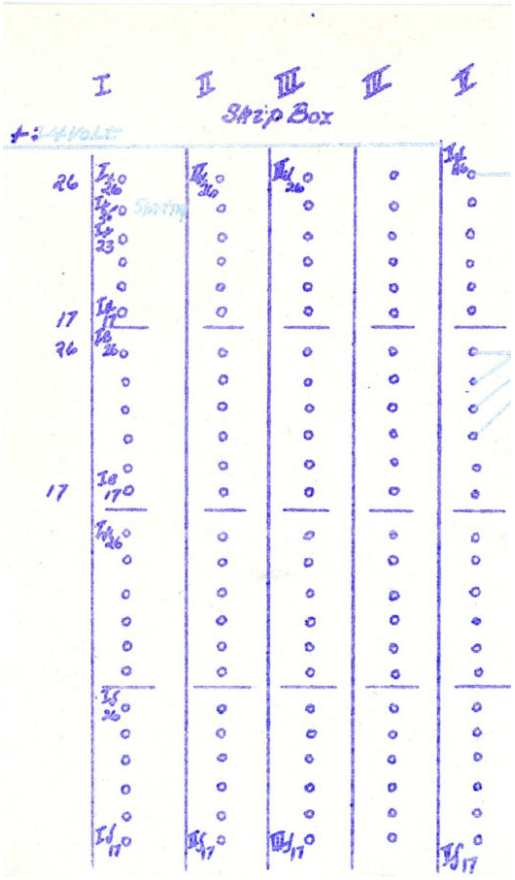

Figure 3. Excerpt from DF 114 showing a schematic view of the skip box. Note the set of six circles representing the six wheels of the M-209. The smallest wheel had 17 letters and the largest 26 which is seen in the annotation of the schematic.

Weber describes his machine as consisting of two boxes. DF 114 does not describe the physical properties of the complete machine but mentions that it consists of three major functional parts. This is not necessarily a contradiction since more than one functional part could be housed in one physical box. In fact, Weber describes one box containing both the relays and the rollers which matches the "skip box" and "switching device" described in DF 114.

A difference worth pointing out is that Weber mentions four rotating rollers but DF 114 counts to five cylinders. Both DF 114 and Weber describe the cylinders having 26 slots where metal lugs could be inserted. This is a detail that is identically described by both sources. The use of light bulbs and relays are also consistent with both sources.

All in all, the similarities between the devices described by Weber and DF 114 are convincing. Both functionally and technically the similarities are many. The few differences that are present are not surprising, considering that the reports about this machine are certainly not error-free.

8 Comparison with the Turing Bombe

The Weber machine is an electromechanical device, just like the Turing Bombe (Turing 2014). It also contains some components that are used in the same way. The Turing Bombe was an electromechanical machine which was used as a tool to help break the German Enigma cipher. The Turing Bombe iterates through a part of the key-space, namely the different Enigma wheel starting positions. For each such position a test is made in order to see if that particular starting position can be ruled out given the current message and crib. If a starting position can not be ruled out, then this position together with some additional output is manually processed further using other types of machines. The Turing Bombe does not output deciphered text but is rather a tool used as part of the deciphering process.

This is similar to the description of Weber's device which was used as a tool to produce the absolute setting given that you already have produced the relative settings. DF 114 further specifies that the device used up to five messages in depth to perform its work.

According to DF 114, the device contains a number of test circuits connected in series, one for each of the six wheels of the M-209. Input from the supposed relative settings are sequentially input through these test circuits and if the test current is able to pass through all six test circuits then a possible solution has been found and a light bulb is switched on. This is similar to how the Turing Bombe uses a test circuit through its drums in order to find a possible solution.

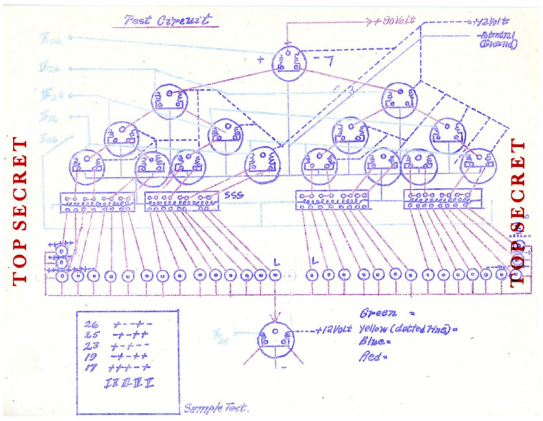

Figure 4. Excerpt from DF 114 showing a test circuit. The test circuit consists of relays connected to form a binary tree into which a test current is injected.

DF 114 describes the use of an electro-mechanical component used to distribute an electric signal sequentially to different outputs. It consists of a rotating arm with carbon contacts bridging two different conductive surfaces. As the arm rotates the pair of conductive surfaces are changed, thus connecting the input to different outputs. A similar solution is used in the US Navy Bombe to generate electrical signals that are synchronized with the mechanical parts of the Bombe (Navy Department 1946).

9 Conclusion

The Weber machine can be named in one breath with World War 2 codebreaking devices such as the Cyclometer, the Bomba, the Turing Bombe, the Desch Bombe, Heath Robinson, Colossus, and the Nightingale. Contrary to the systems mentioned, the Weber machine was constructed by the Germans (Dahlke 2020). The aim of this paper is to provide additional information about this system.

To the regret of the authors, it is still not known how the Weber machine worked. Apparently, the authors of the documents used in this work did not understand this device, either. To close this gap, unfortunately, Reinold Weber can't be asked any more – he died in 2021. Additional sources might exist, and it seems possible to retrieve more information from the TICOM documents referenced in this work, including the figures, which are often difficult to understand. The authors welcome any advice.

Apart from this, a possible way to conclude this device's functioning is to write a computer simulation of it and use real M-209 messages in depth to recover some relative settings that can be used to test the simulation and hence the device. However, writing such a simulation is clearly a difficult task. It would have to be done in stages, trying out various theories about the exact working of the machine.

Acknowledgments

We would like to thank the reviewers of this paper, particularly "Reviewer 1", who provided excellent comments and additional information. We also would like to thank Paul Reuvers and Marc Simons from the Crypto Museum (cryptomuseum.com) for permitting us to use their M-209 photograph, as well as Marek Grajek for shepherding this publication.

References

T. R. W. Burton Miller et al. 1950. Special Conference on M-209 Security. https://www.nsa.gov/Portals/75/documents/news-features/declassified-documents/friedman-documents/patent-equipment/FOLDER_371/41755249079440.pdf.

Carola Dahlke. 2020. The Auxiliary Devices of OKW/Chi. HistoCrypt 2020, Proceedings of the 3rd International Conference on Historical Cryptology.

Otto Leiberich. 1999. Vom diplomatischen Code zur Falltürfunktion. Hundert Jahre Kryptographie in Deutschland. *Spektrum der Wissenschaft*, 6, 26-34.

Navy Department. 1946 *Technical and Theoretical Report of N-530 Bombe*. Navy Department, Washington D.C.

Alfred Pokorn. 1950. *Pfadfinder-Handbuch*. Pfad-Verlag, Salzburg.

Alfred Pokorn. 1964. *Apatschen-Indianer*. Oldenbourg, Munich.

Paul Reuvers and Marc Simons. 2022a. Crypto AG. https://www.cryptomuseum.com/crypto/hagelin.

Paul Reuvers and Marc Simons. 2022b. M-209. https://www.cryptomuseum.com/crypto/hagelin/m209.

Randy Rezabek. 2017. *TICOM: the Hunt for Hitler's Codebreakers*. independently published, Rochester, NY.

Klaus Schmeh. 2015. *Wie ein Rätsel der Kryptologie-Geschichte nach 70 Jahren gelöst wurde*. https://scienceblogs.de/klausis-krypto-kolumne/2015/07/04/wie-ein-raetsel-der-kryptologie-geschichte-nach-70-jahren-geloest-wurde/.

Klaus Schmeh. 2004. *Als Codeknacker im zweiten Weltkrieg*. https://www.heise.de/tp/features/Als-deutscher-Code-Knacker-im-Zweiten-Weltkrieg-3436447.html.

Klaus Schmeh. 2022. *Codeknacker gegen Codemacher*. Springer, Heidelberg. 362-364.

TICOM 1945a. *Consolidated Report on Information Obtained from PW Erdmann, Grübler, Hempel, Karrenberg, Schmitz, Suschowk*. C.S.D.E.I.C. (U.K.), S.I.R. 1717.

TICOM 1945b. *Report by Alfred Pokorn, of OKH/CHI, on M-209*. TICOM Document 2785.

J. C. Barret. 1943. *Signal Operation Instructions*. 84th Infantry Division, 34-45.

TICOM. 1946. *Volume 4 Signal Intelligence Service of the Army High Command*. WDGAS-14, 20-41.

TICOM. 1948a. *German Cryptanalytic Device for Solution of M-209 Traffic*. TICOM Document 2785, DF 114. NARA, NAID: 23889821. https://catalog.archives.gov/id/23889821.

TICOM. 1948b. *Report on The Solution of Messages in Depth of The American Cipher Device M-209*. TICOM Document 2794, DF 120. NARA, NAID: 23889823. https://catalog.archives.gov/id/23889823.

TICOM. Undated. *Determination of the Absolute Setting of the AM-1 (M-209) by Using Two Messages with Different Indicators*. TICOM Document 2795, DF 105. NARA, NAID: 26466553. https://catalog.archives.gov/id/26466553.

Christos Triantafyllopoulos. 2017. *Christos military and intelligence corner*. http://chris-intel-corner.blogspot.com/2017/02/the-compromise-of-croat-enigma-k-cipher.html.

Dermot Turing. 2014. *Demystifying the Bombe*. The History Press, Stroud.

War Department. 1944. *Converter M-209, M-209-A, M-209-B (cipher)*. U.S. War Department.